SSL Report: fao.ge.ch (160.53.186.45)

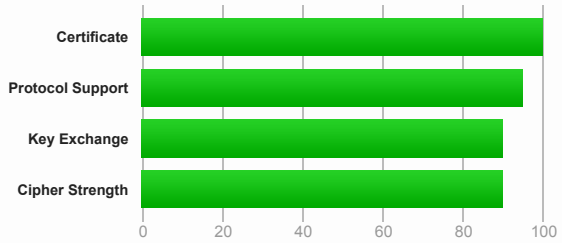
Assessed on: Tue, 21 Mar 2017 08:16:11 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A-



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

The server does not support Forward Secrecy with the reference browsers. Grade reduced to A-. MORE INFO »

Server sent invalid HSTS policy. See below for further information.

Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.ge.ch Fingerprint SHA1: 9910bbaeffac4f9a6da138f7fc9fead810b3017b Pin SHA256: v1M1lkl0SDGKRqYAzkJUE4wbSVL2yQ0rxCqryNtqoXs=
Common names	*.ge.ch
Alternative names	*.ge.ch ge.ch
Valid from	Mon, 30 Nov 2015 10:12:06 UTC
Valid until	Fri, 30 Nov 2018 10:12:06 UTC (expires in 1 year and 8 months)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	SwissSign Server Gold CA 2014 - G22 AIA: http://swisssign.net/cgi-bin/authority/download/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.swisssign.net/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE OCSP: http://gold-server-g2.ocsp.swisssign.net/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE
Revocation status	Good (not revoked)
DNS CAA	No
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	3 (5077 bytes)
Chain issues	Contains anchor

#2

Subject	SwissSign Server Gold CA 2014 - G22 Fingerprint SHA1: adf2897316718b4525ce370082d9f123d4938f98 Pin SHA256: skyozdmp140ljrHvjRijq3v2/yQ1nyfFyBiA9uOKuw8=
Valid until	Sat, 15 Sep 2029 14:09:12 UTC (expires in 12 years and 5 months)

Additional Certificates (if supplied)

Key	RSA 2048 bits (e 65537)
Issuer	SwissSign Gold CA - G2
Signature algorithm	SHA256withRSA

#3

Subject	SwissSign Gold CA - G2 In trust store Fingerprint SHA1: d8c5388ab7301b1b6ed47ae645253a6f9f1a2761 Pin SHA256: QPz8KlddzL/ry99s10MzEtpjxO/PO9extQXClCCuAnQ=
Valid until	Sat, 25 Oct 2036 08:30:35 UTC (expires in 19 years and 7 months)
Key	RSA 4096 bits (e 65537)
Issuer	SwissSign Gold CA - G2 Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

TLS 1.1 (suites in server-preferred order)

TLS 1.0 (suites in server-preferred order)

TLS 1.0 No SNI (server has no preference)

Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 No FS RC4
Android 4.0.4	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS

Handshake Simulation

Android 4.3	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Android 5.0.0	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 6.0	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Android 7.0	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Baidu Jan 2015	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Chrome 51 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 49 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Googlebot Feb 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256 No FS
IE 6 / XP No FS [1] No SNI [2]	Server closed connection		
IE 7 / Vista	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS [1] No SNI [2]	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 RC4
IE 8-10 / Win 7 R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 10 / Win Phone 8.0	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Edge 13 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Java 6u45 No SNI [2]	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 No FS RC4
Java 7u25	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u31	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2e R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Supported**

Protocol Details

Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	**With some browsers** (more info)
ALPN	No
NPN	No
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Invalid** Failed to parse header ���max-age=31536000���
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported EC Named Curves	secp256r1
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://fao.ge.ch/** (HTTP/1.1 302 Moved Temporarily)

2 **https://fao.ge.ch/captcha?t=33d6393659b667910f5f4cd25f6c63a8** (HTTP/1.1 301 Moved Permanently)

3 **https://fao.ge.ch/captcha/?t=33d6393659b667910f5f4cd25f6c63a8** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Tue, 21 Mar 2017 08:13:34 UTC
Test duration	157.460 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	demoeduidp.ge.ch

SSL Report v1.27.3